

## Is Eve listening? An Interactive Learning Tool Designed to Teach Quantum Communication

Yan A. Chagas<sup>1\*</sup>, Lorena R. Cerutti<sup>1,2</sup>, Isadora R. A. Mello<sup>1,3</sup>, Marcelo A. Moret<sup>1</sup>

<sup>1</sup>QuIIN - Quantum Industrial Innovation, EMBRAP II CIMATEC Competence Center in Quantum Technologies, SENAI CIMATEC University; Salvador, Bahia; <sup>2</sup>Santa Catarina State University, Department of Physics; Joinville, Santa Catarina;

<sup>3</sup>Federal University of Paraná, Department of Physics; Curitiba, Paraná, Brazil

**This study proposes an alternative approach to foster student engagement in the educational process by encouraging autonomy and active participation. Game-based elements are employed to introduce topics in modern physics to basic education students, with a focus on fundamental concepts of quantum cryptography. Specifically, the didactic material developed presents the core principles and operation of the BB84 protocol. To facilitate understanding, a board game was created simulating the initial steps of the protocol, including the presence of an eavesdropper attempting to intercept the message.**

**Keywords:** Active Learning Methodologies. Gamification. Board Game. Quantum Cryptography. BB84. **Abbreviations:** Active Learning Methodologies, ALMs. Quantum Computing, QC. Quantum Information, QI. Quantum Key Distribution, QKD.

In Brazil, education is regarded as a fundamental human right, with access and free provision guaranteed by the Federal Constitution [1] and recognized by the Universal Declaration of Human Rights [2]. Nevertheless, low levels of school learning underscore the challenges of promoting transformative, free, and high-quality education in contemporary society. Although essential, investments in public policies aimed at the structural improvement of educational institutions alone are not sufficient to ensure quality education [3]. Reforms in basic education involve developing students' interest in content, and to this end, adaptations in teaching methodologies are necessary, along with a curriculum overhaul [4].

Active learning methodologies (ALMs) position the teacher as a facilitator, fostering collaboration, autonomy, and problem-based knowledge building [5]. As a new paradigm of educational quality, they integrate real-world situations and innovations into the learning process [6]. Common approaches include project-based learning, the flipped

classroom, and gamification [5].

However, developing approaches that encourage students to take responsibility for their learning can become a fruitless endeavor if the content taught in the classroom is presented in an isolated or fragmented manner—disconnected from its social and productive context [7]. In this scenario, it is essential to highlight the need for a comprehensive curriculum reform in the context of physics education. This need arises from the fact that the current curriculum is predominantly composed of concepts developed before the 20th century [4], placing greater emphasis on classical physics while neglecting modern and contemporary physics [8]. Such an approach is unwarranted, as excluding theories like relativity and quantum mechanics [9] deprives students of the opportunity to understand the technologies and societal debates that shape their everyday lives [8].

In the field of technology, the pursuit of greater computational processing power has driven the development of quantum computing (QC) and quantum information (QI) [10], which (alongside advances in artificial intelligence) is reshaping industrial processes and contributing to the emergence of the Fourth Industrial Revolution [9].

As scientific and commercial interest in these technologies grows, the media has become saturated with concepts that often appear abstract

Received on 6 April 2026; revised 22 July 2026.

Address for correspondence: Yan A. Chagas. SENAI CIMATEC University. Av. Orlando Gomes 1845, Piatã, Salvador – BA – Brazil, Zipcode: 41650-010. E-mail: yan.chagas@fieb.org.br.

J Bioeng. Tech. Health 2026;9(8):847-853  
© 2026 by SENAI CIMATEC University. All rights reserved.

to the general public [4]. In the case of QC and QI, it is common to find articles and news reports discussing the impact of quantum technologies on strategic sectors of society, such as healthcare, cryptography, and data security [9].

In this context, the relevance of technological literacy has once again come to the forefront, giving rise to a new educational movement focused on fostering scientific literacy in the field of quantum science. Intending to engage students and prepare them to understand the technologies underlying the second quantum revolution, we have developed an educational resource grounded in gamification and centered on concepts from modern physics.

Assuming that Generation Alpha consists of digital natives [5], this study proposes the creation of a card game based on the BB84 quantum cryptography protocol. The objective is to use an active learning methodology to make these complex concepts more accessible to students, encouraging collaborative problem-solving through peer interaction. As a result, we aim to foster the development of cognitive skills, such as analysis and synthesis, rather than merely memorizing content [6]. In the following sections of this article, gamification will be presented as an active pedagogical approach, and both the BB84 protocol and the mechanics of the developed game will be discussed in detail.

## Materials and Methods

With the growing search for alternatives to the traditional teaching model and based on the remarkable ability of games to capture and sustain participants' attention, both the demand for and the development of research on gamification in educational settings have increased, highlighting it as an effective strategy in the teaching and learning process [8,11,12]. By definition, gamification involves adopting a game-like mindset, applying game mechanics and aesthetics in educational and non-playful contexts [5,8,11]. The purpose of this approach is clear: to motivate students, sustain their attention, and foster problem-solving skills, thereby reframing the learning process [5,8,11].

The use of educational games can also be understood as a simulation of a real-world situation, in which the student (while perceiving themselves as playing) is actively appropriating concepts. For such activities to be effective, certain fundamental game components, such as objectives and rules, must be clearly and precisely defined. It is essential to note that a poorly formulated or overly complex objective may compromise the activity's success; in such cases, it should be broken down into smaller, more manageable parts [11]. Similar care must be taken when defining the rules, as they determine the procedures to be followed by players and structure the actions required to complete the challenge [11,12].

In the following subsection, we provide a brief explanation of the importance of cryptography for human development and the BB84 protocol, to support educators responsible for implementing the activity, helping them understand both its development context and its fundamental concepts.

### A Brief Review of Cryptography

One of the earliest pieces of evidence of cryptography in human history was found in Egypt, where unconventional hieroglyphs were used in place of the usual symbols and carved on the walls of a tomb in 1900 BC [13]. Cryptography, from Greek, means hidden writing. The origin of the word is attributed to the Spartans, who used a wooden baton, also known as scytale, to conceal their messages [14]. Only those who had the scytale of the correct dimension and format were able to decipher the message.

Another well-known record dates back to 100 BC, when the Roman emperor Julius Caesar, to communicate securely with the Roman army, used a cryptographic system in which each character of the message was replaced by another, based on a key. This type of encryption technique became known as the Caesar Cipher [15], a monoalphabetic rotation whereby each letter of the alphabet was replaced by the third successive letter. That is, A became D,

B became E, and so on. As an example, the word CRYPTOGRAPHY, using this logic, would become FUBSWRJUDSKB.

In contemporary history, World War I opened new doors for the development of modern cipher systems, which advanced with the rise of military communication via radio [15]. The ease of intercepting radio signals made encryption essential, but ciphers like the Caesar Cipher were relatively easy to break due to the high message volume.

In the post-war period, the Enigma cryptographic machine was developed by the German engineer Arthur Scherbius and was later used by the Nazi regime during World War II [15]. Enigma's daily reconfigurable rotor made it hard to break, with Alan Turing's work on its code aiding the Allies and paving the way for modern computing. As communication technology advances, cryptography must evolve to protect data, a challenge heightened by the rise of quantum computers. With a quantum computer, classical cryptography could be easily broken due to the significantly higher processing power compared to today's computers [14].

As a result, new quantum cryptography protocols have begun to appear, protocols that would remain secure even against cyberattacks using a quantum computer. These protocols are based on the laws of quantum mechanics, unlike post-quantum cryptography, which is based on classical physics but is designed to be resistant to both classical and quantum computers [13].

Quantum cryptography, rooted in modern physics, can be taught in physics, mathematics, history, and ethics, linking quantum mechanics, probability, historical uses of cryptography, and debates on privacy in the technological era.

### BB84 Protocol

Originally proposed in 1984 by Charles Bennett and Gilles Brassard, the BB84 protocol (named after its creators and the year of its conception) is currently one of the most well-known quantum key distribution (QKD) protocols [16]. It is

characterized by the use of quantum properties (specifically, the polarization states of photons) to enable cryptographic key exchanges that are theoretically unbreakable [17, 18]. The protocol involves three main actors: Alice, Bob, and Eve (short for eaves-dropper) [18]. For clarity, this paper will present the operation of the BB84 protocol in a series of distinct stages.

In the first stage, Alice transmits information to Bob through a quantum channel. To achieve this, she sends a sequence of individually polarized photons, each randomly prepared in one of two bases: the orthogonal basis (+), or the diagonal basis ( $\times$ ). In the orthogonal basis, photons are polarized at either  $0^\circ$  or  $90^\circ$ , while in the diagonal basis, they are polarized at  $\pm 45^\circ$  [18]. Bits are then encoded by arbitrarily associating logical values with the polarization states of the photons [17,18]. To visualize the photon transmission and measurement bases. In this work, we adopt the convention of assigning bit 0 to photons polarized at  $0^\circ$  or  $+45^\circ$ , and bit 1 to photons polarized at  $90^\circ$  or  $-45^\circ$ .

Bob then randomly selects the basis on which to measure the received photons [17]. If the measurement basis matches the transmission basis, Bob retrieves the correct bit; otherwise, the result is entirely random [18]. The sequences of bits sent by Alice and received by Bob form what is known as the raw key [18]. Due to the random basis selection, an intrinsic error rate of approximately 25% is expected even in the absence of eavesdropping, which leads to discrepancies between Alice's and Bob's raw keys [18].

The second stage of the protocol, referred to as the reconciliation phase, occurs over a classical public channel. At this stage, Alice reveals the polarization bases used for each photon, without disclosing the corresponding bit values [18,17]. Based on this information, Bob compares the sequence of bases he used and discards all bits resulting from measurements made with mismatched bases. The key formed from the remaining, correctly measured bits is referred to as the sifted key [18, 17].

The final three stages of the BB84 protocol focus on Eve detection and error correction. In the third

stage, Alice and Bob compare a random subset of the bits that were sent and measured to estimate the error rate. The quantum bit error rate (QBER) serves as an indicator of the presence or absence of an eavesdropper [17,18]. Because the bits sent by Alice may undergo rotation during transmission or be incorrectly measured by Bob due to basis misalignment, an intrinsic error rate related to channel quality is expected [17]. Error rates exceeding this expected threshold are interpreted as additional errors introduced in the transmission, typically attributed to Eve attempt to intercept information.

If Alice and Bob obtain results that indicate the presence of a third party in the process, they must terminate the key transmission to ensure the security of the transmitted information. Alice must then generate a new sequence of polarized photons using random bases, effectively restarting the protocol. Otherwise, if the communication is considered sufficiently secure, the bits used during verification are discarded, and both the sender and the receiver proceed to the final two steps of the protocol [17].

Steps four and five of the BB84 protocol involve the application of algorithms designed to minimize noise originating from the communication channel and equipment (thus reducing the error rate in the bits received by Bob), as well as to amplify privacy. It is important to note that these final three steps result in a significant reduction in key size, that is, the number of photons emitted by Alice must be substantially greater than the final desired key length [18].

## Results and Discussion

The proposal to develop a board game (Figure 1) focused on teaching quantum communication is justified by the difficulty in finding educational materials specifically tailored to this subject. Although several games address concepts related to quantum mechanics, QC, and QI [19], few are specifically designed for classroom application. When searching is limited to games available

in Portuguese, this gap becomes even more pronounced, with a significant reduction in the availability of accessible resources. Given Brazil's educational inequalities and limited Internet access in many schools [20], board games offer an affordable and accessible alternative to digital resources that align with curricular objectives. The proposed game simulates the initial stages of the BB84 quantum key distribution protocol, using custom dice to represent quantum states, measurement bases, and intercept attempts. This playful approach helps students grasp core quantum concepts like randomness and probability by immersing them in a dynamic, hands-on experience.

To be able to play, we need the following items, 60 States Cards (bits 0 or 1); 40 cards of bases base ( $0^\circ$ ,  $-45^\circ$ ,  $45^\circ$  and  $90^\circ$ ); 20 Alice's Base Cards - 05 per base ( $0^\circ$ ,  $90^\circ$ ,  $-45^\circ$ ,  $45^\circ$ ); 6 dice of base and states (the faces show + or  $\times$ , and 0 or 1); 1 dice of "intercept or not intercept"; 3 card board of States and Bases and player's shield.

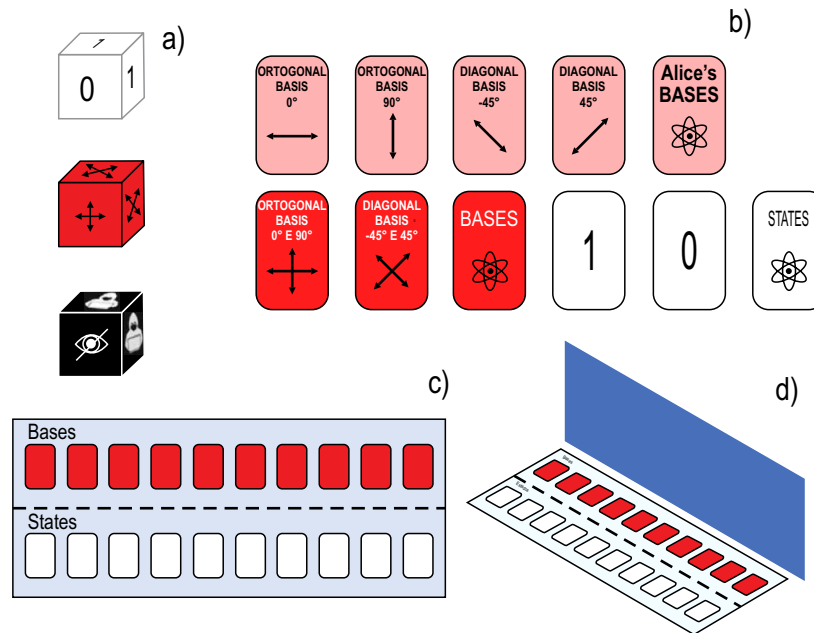
## Game Rules

With the kit in Figure 1, two game modes can be implemented. The first, with Alice and Bob, demonstrates the protocol's basic operation, similar to a didactic computer simulation but using game elements. The second, with Alice, Bob, and Eve, assigns different goals: Alice and Bob aim to transmit a secure key, while Eve tries to intercept it.

Each player chooses who will be Alice, Bob, and Eve. Everyone gets a board and a shield to hide it, plus a state die and a basis die (Eve also gets an extra interception success die). Each player has 10 bit-0 cards and 10 bit-1 cards; Alice receives special state cards, while Bob and Eve get 5 cards for each basis (orthogonal and diagonal).

Alice starts by creating the sequence to be transmitted, rolling the two dice (basis and state) to determine the basis and state for each round. This repeats for 10 rounds, where Alice selects one basis card and one compatible state card, placing on their respective boards. Although the state dice are identical, Alice has four possible state card choices

**Figure 1.** Game Elements: a) The white die is the states' dice, the red die is the bases dice, and the black die is the interception success die. b) The status cards are in red, differentiating those used by Alice and the others by Bob and Eve. c) The board. d) The player's shield.



(two per basis) and must select one compatible with the die's basis. As established in section II.B, some combinations cannot be transmitted. This limitation can help detect intruders, serve as a discussion topic, or be addressed beforehand with transmission guidelines, at the instructor's discretion.

Next, Eve tries to intercept the message: she secretly rolls two dice (basis and interception success) and reveals the result only to Alice. If Eve gets "intercept" and the basis matches Alice's, she obtains the bit and Alice reveals the value. Otherwise, Eve rolls the state die and records a random value.

Bob now receives the data. He rolls the basis die. For rounds without Eve's interception, Alice checks if bases match; if states also match, she tells Bob to place bit-1 or bit-0. Otherwise, Bob rolls the state die to set the bit. In intercepted rounds, Eve decides Bob's basis and state. After 10 rounds, verification begins. Shields are removed, cards revealed. Alice and Bob keep only bits where bases match; Eve keeps only bits she successfully intercepted. If Eve forwarded the state to Bob without detection in at least three rounds, she wins. If Alice and

Bob communicate securely or detect and discard the compromised protocol, they win. In the initial rules, re-transmission and eavesdropping detection are left out to encourage players to create their own security strategies and better understand how the protocol works. Just like in real protocols, if the error rate reaches 25% or more, the channel is considered compromised. In the game, this means Eva must successfully intercept at least three out of ten rounds, equivalent to 30% of the key. The choice of 10 rounds makes percentage calculations easier, and the teacher can decide whether all rounds are played by each player at once or if turns alternate bit by bit.

Students should understand that the computational process requires more formalism than the game dynamic, which aims only to give a general intuition of the BB84 protocol. In the actual protocol, Alice and Bob communicate via an authenticated classical channel: Alice informs the bases used, Bob compares results and discards discrepancies, while Eve only intercepts and resends photons. If the error rate exceeds the limit, the channel is deemed compromised.

To enrich the activity, steps can include converting the final key from binary to text to decrypt a message, creating a narrative context, or varying key lengths to analyze the difficulty of detecting an eavesdropper, enabling interdisciplinary discussions.

In the mode game with Alice and Bob only, Eve's mechanics are removed. Both cover their boards, keep the same base/state cards and dice. Alice rolls both dice, records the results, and Bob rolls the base die. If bases match, Alice tells Bob the state; otherwise, he rolls the state die. At the end, unmatched bases are discarded and remaining states analyzed for possible intrusion.

The dynamic can be simplified by change custom dice with regular dice or coins, defining 'heads' and 'tails' for each parameter, or by using playing cards with rules based on suits, parity, or other rules, while preserving the proposal's simplicity and focus on playful concept building.

## Conclusion

This work represents a starting point for future didactic applications involving quantum technologies in basic education, proposing a board game to simulate the BB84 protocol, highlighting gamification as an effective tool to engage students through playful and didactic methods. Given the growing global demand for quantum professionals, introducing these topics early in schooling is both relevant and strategic, especially for exact sciences with low enrollment and high dropout rates. Besides enhancing student learning, the proposal supports curriculum updates and teacher development. Next, we plan to implement this resource in classrooms to gather data on the effectiveness of gamification in teaching quantum technology concepts.

## Acknowledgments

This work has been fully funded by the project "iNOVATeQ Lato Senso Especialização em Computação Quântica - Pesquisador - QIN-FCRH-2024-1-2-2" in supported by QuIIN - Quantum Industrial Innovation, EMBRAPPII

CIMATEC Competence Center in Quantum Technologies, with financial resources from the PPI IoT/Manufatura 4.0 of the MCTI grant number 053/2023, signed with EMBRAPPII.

## References

1. Brasil. Constituição da República Federativa do Brasil de 1988. Capítulo III, Seção I, Art. 205. Brasília (DF): Brasil; 1988.
2. United Nations. Universal Declaration of Human Rights. Article 26. New York: United Nations; 1948.
3. Rocha CN, Novaes AMP, Avelar KES. Análise do desempenho da educação brasileira baseada nos indicadores locais PISA e IDEB. *LexCult*. 2020;4(3):71-92.
4. Silva JMC. Transposição didática da computação quântica: estados emaranhados e teleporte quântico [master's thesis]. Araguaína (TO): Universidade Federal do Norte do Tocantins; 2022.
5. Cunha MB, Omachi NA, Ritter OMS, Nascimento JE, Marques GQ, Lima FO. Metodologias ativas: em busca de uma caracterização e definição. *Educ Rev*. 2024;40.
6. Maia MC. Resenha: entendendo a necessidade de renovação no processo de ensino e aprendizagem. *Rev Adm Empres Eletrônica*. 2010;9(1).
7. Albuquerque AG. A importância da contextualização na prática pedagógica. *Res Soc Dev*. 2019;8(11):1-13.
8. Sampaio WS, Frota DA. Conceitos de mecânica quântica para o ensino médio por meio de um jogo de tabuleiro. *Rev Ensino Debate*. 2024;2.
9. Oikonomou AV, Savvas IK, Iatrellis O. Enhancing quantum literacy with quantum key distribution: a study with secondary education school students. *Preprints*. 2025.
10. Cerutti LR. Caminhadas quânticas desordenadas com barreira absorvedora [master's thesis]. Joinville (SC): Universidade do Estado de Santa Catarina; 2023.
11. Silva JB, Sales GL, Castro JB. Gamificação como estratégia de aprendizagem ativa no ensino de física. *Rev Bras Ensino Fís*. 2019;41(4).
12. Studart N. A gamificação como design instrucional. *Rev Bras Ensino Fís*. 2022;44.
13. IBM. The history of cryptography [Internet] 2025. Available from: IBM website.
14. Louridas P. A history of cryptography from the Spartans to the FBI [Internet]. MIT Press Reader. 2025.
15. Singh S. The code book: the science of secrecy from ancient Egypt to quantum cryptography. New York: Doubleday; 1999.
16. Reddy MSK, Mohan BC. Comprehensive analysis of BB84, a quantum key distribution protocol. *arXiv [Preprint]*. 2023.
17. Camargo ALP, Pereira LO, Balthazar WF, Huguenin JAO. Simulação do protocolo BB84 de criptografia

- quântica utilizando um feixe laser intenso. Rev Bras Ensino Fís. 2017;39(2).
18. Marquezino FL. Estudo introdutório do protocolo quântico BB84 para troca segura de chaves [undergraduate thesis]. Rio de Janeiro: Centro Brasileiro de Pesquisas Físicas.
  19. Piispanen L, Pfaffhauser M, Wootton J, et al. Defining quantum games. EPJ Quantum Technol. 2025;12:7.
  20. Jornal Nacional, Rede Globo. Falta de laboratórios e de treinamento para professores atrasa preparo de alunos para mundo digital nas escolas brasileiras [Internet]. G1. 2025 Jan.